

Some properties of finite meadows

Inge Bethke^{a,1,*} Piet Rodenburg^{a,2}

^a*University of Amsterdam, Faculty of Science, Section Theoretical Software
Engineering (former Programming Research Group)*

Key words: combinatorial problems, data structures, specification languages.

1 Introduction

In abstract algebra, a field is a structure with total operations of addition, subtraction and multiplication. Moreover, every element has a multiplicative inverse—except 0. In a field, the rules hold which are familiar from the arithmetic of ordinary numbers. The prototypical example is the field of rational numbers. Fields can be specified by the axioms for commutative rings with identity element (*CR*, see Table 1), and the negative conditional formula

$$x \neq 0 \rightarrow x \cdot x^{-1} = 1,$$

which is difficult to apply and automate in formal reasoning.

The theory of fields is a very active area which is not only of great theoretical interest but has also found applications both within mathematics—combinatorics and algorithm analysis—as well as in engineering sciences and, in particular, in coding theory and sequence design. Unfortunately, since fields are not axiomatized by equations only, Birkhoff’s Theorem fails, i.e. fields do not constitute a variety: they are not closed under products, subalgebras, and homomorphic images.

In [2], it is proved that there exists a finite equational specification under initial algebra semantics—without hidden functions—of the rational numbers with field operations that are all total. Subsequent investigations led to the concept

* Corresponding author. Address: Kruislaan 403, 1098 SJ Amsterdam, The Netherlands

¹ E-mail: inge@science.uva.nl

² E-mail: pietr@science.uva.nl

(CR)	$(x + y) + z = x + (y + z)$
	$x + y = y + x$
	$x + 0 = x$
	$x + (-x) = 0$
	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
	$x \cdot y = y \cdot x$
	$x \cdot 1 = x$
	$x \cdot (y + z) = x \cdot y + x \cdot z$
(Ref)	$(x^{-1})^{-1} = x$
(Ril)	$x \cdot (x \cdot x^{-1}) = x$

Table 1

Specification of the theory of meadows

of *meadows* which are very similar to fields—the considerable difference being that meadows do form a variety.

A meadow is a commutative ring with identity element (CR) equipped with a total unary operation $^{-1}$, *inversion*, which satisfies the equation for *reflection* (Ref) and the *restricted inverse law* (Ril) . That is, a meadow is specified by the set of axioms in Table 1. All fields and products of fields can be viewed as meadows—basically by stipulating $0^{-1} = 0$ —but not conversely. Also, every commutative Von Neumann regular ring (see e.g. [5]) can be expanded to a meadow (cf. [1]).

Example 1.1 Consider the ring $\mathbb{Z}/10\mathbb{Z}$ with elements $\{0, 1, 2, \dots, 9\}$ where arithmetic is performed modulo 10. Here

$$\begin{array}{ll}
(0)^{-1} = 0 & (1)^{-1} = 1 \\
(2)^{-1} = 8 & (3)^{-1} = 7 \\
(4)^{-1} = 4 & (5)^{-1} = 5 \\
(6)^{-1} = 6 & (7)^{-1} = 3 \\
(8)^{-1} = 2 & (9)^{-1} = 9
\end{array}$$

Since the inversion is an involution which also satisfies *Ril*, this ring is also a meadow.

The aim of this note is to describe the structure of finite meadows. We will show that the class of finite meadows is the closure of the class of finite fields

under finite products. As a corollary, we obtain a unique representation of minimal meadows in terms of prime fields.

2 Decomposition of finite meadows

In [3] it is proved that every commutative regular ring in the sense of von Neumann is a subdirect union of fields. In this section we show that every finite meadow is a direct product of finite fields. Part of the proof is also known from the theory of rings: under certain conditions—also met in our case—a ring R can be decomposed as $R = e_1 \cdot R \cdot e_1 \oplus \dots \oplus e_n \cdot R \cdot e_n$ where $\{e_1, \dots, e_n\}$ is the set of mutually orthogonal minimal idempotents in R (see e.g. [4]).

Definition 2.1 *Let M be a meadow.*

- (1) *An element $e \neq 0$ in M is an idempotent if $e \cdot e = e$.*
- (2) *If $e, e' \in M$ are idempotents then we write $e \leq e'$ if $e \cdot e' = e$.*
- (3) *An idempotent $e \in M$ is minimal if for every idempotent $e' \in M$,*

$$e' \leq e \Rightarrow e' = e.$$

Proposition 2.2

Let M be a meadow and $e \in M$ an idempotent. Then

- (1) *$e = e^{-1}$*
- (2) *$e \cdot M$ is a meadow with multiplicative identity element e .*
- (3) *If e is minimal then $e \cdot M$ is a field with multiplicative identity element e .*

Proof:

- (1) Since in every meadow inversion distributes over multiplication (see [1]) we have

$$e = e \cdot e \cdot e^{-1} = e \cdot e^{-1} = e \cdot (e \cdot e)^{-1} = e \cdot e^{-1} \cdot e^{-1} = e^{-1}.$$

- (2) Since idempotents are self-inverse $e \cdot M$ is closed under $+$, \cdot , $^{-1}$ and clearly satisfies the axioms for meadows.
- (3) Since $e \cdot M$ is a meadow with multiplicative identity element e , it suffices to prove that $(e \cdot m) \cdot (e \cdot m)^{-1} = e$ for every $e \cdot m \neq 0$. Thus let $e \cdot m$ be a nonzero element. Then $(e \cdot m) \cdot (e \cdot m)^{-1} \neq 0$ because otherwise

$$e \cdot m = (e \cdot m) \cdot (e \cdot m) \cdot (e \cdot m)^{-1} = 0.$$

Moreover,

$$(e \cdot m) \cdot (e \cdot m)^{-1} \cdot (e \cdot m) \cdot (e \cdot m)^{-1} = (e \cdot m) \cdot (e \cdot m)^{-1}.$$

So $(e \cdot m) \cdot (e \cdot m)^{-1}$ is an idempotent. Hence, since

$$e \cdot (e \cdot m) \cdot (e \cdot m)^{-1} = (e \cdot m) \cdot (e \cdot m)^{-1}$$

and e is minimal we have $(e \cdot m) \cdot (e \cdot m)^{-1} = e$.

□

The main properties of idempotents are summarized in the following proposition.

Proposition 2.3

Let M be a meadow.

- (1) \leq is a partial order on the idempotents.
- (2) If $e, e' \in M$ are idempotents and $e \cdot e' \neq 0$ then $e \cdot e'$ is also an idempotent.
- (3) If $e, e' \in M$ are idempotents and $e < e'$ then $e' - e$ is also an idempotent.

Proof:

- (1) Clearly \leq is reflexive. If $e \leq e'$ and $e' \leq e''$ then

$$e \cdot e'' = (e \cdot e') \cdot e'' = e \cdot (e' \cdot e'') = e \cdot e' = e.$$

Therefore the relation is transitive. Finally, if $e \leq e'$ and $e' \leq e$ then

$$e = e \cdot e' = e' \cdot e = e'.$$

Thus \leq is also antisymmetric.

- (2) We multiply $e \cdot e'$ with itself: $(e \cdot e') \cdot (e \cdot e') = (e \cdot e) \cdot (e' \cdot e') = e \cdot e'$.
- (3) We multiply $e' - e$ with itself:

$$(e' - e) \cdot (e' - e) = e' \cdot e' - e \cdot e' - e' \cdot e + e \cdot e = e' - e - e + e = e' - e.$$

□

Definition 2.4 *Let M be a meadow and $e, e' \in M$. We call e and e' orthogonal if $e \cdot e' = 0$.*

Proposition 2.5

Let M be a meadow.

- (1) If $e, e' \in M$ are different minimal idempotents then e and e' are orthogonal.

(2) If $e, e' \in M$ are orthogonal idempotents then $e + e'$ is an idempotent.

Proof:

- (1) Suppose $e \cdot e' \neq 0$. Then $e \cdot e'$ is an idempotent by Proposition 2.3(2). Moreover, $e \cdot e' = e \cdot e \cdot e' = e \cdot e' \cdot e$, i.e. $e \cdot e' \leq e$. Thus $e \cdot e' = e$, since e is minimal. Likewise $e \cdot e' = e'$ and hence $e = e'$. Contradiction.
- (2) We multiply again:

$$(e + e') \cdot (e + e') = e \cdot e + e \cdot e' + e' \cdot e + e' \cdot e' = e + 0 + 0 + e' = e + e'.$$

Moreover, $(e + e') \cdot e = e \cdot e + e \cdot e' = e$. Hence $e + e' \neq 0$.

□

We now show that every finite meadow is the direct product of the fields generated by its minimal idempotents.

Lemma 2.6

Let M be a finite meadow and $\{e_1, \dots, e_n\} \subseteq M$ be the set of minimal idempotents. Then $e_1 + \dots + e_n = 1$.

Proof: Since minimal idempotents are orthogonal we have $e_i \cdot e_j = 0$ for $i \neq j$ by Proposition 2.5 (1). Therefore for every $1 \leq i < n$, $e_1 + \dots + e_i$ is an idempotent orthogonal with e_{i+1} , and hence $e_1 + \dots + e_n$ is an idempotent by Proposition 2.5 (2). And therefore $1 - (e_1 + \dots + e_n)$ is an idempotent by Proposition 2.3 (3) unless it is 0. Suppose $1 - (e_1 + \dots + e_n)$ is an idempotent. Then, since \leq is a partial order there must be some minimal idempotent $e_i \leq 1 - (e_1 + \dots + e_n)$. But

$$\begin{aligned} e_i \cdot (1 - (e_1 + \dots + e_n)) &= e_i - (e_i \cdot e_1 + \dots + e_i \cdot e_i + \dots + e_i \cdot e_n) \\ &= e_i - (0 + \dots + e_i \cdot e_i + \dots + 0) \\ &= 0 \end{aligned}$$

Contradiction. Hence $1 - (e_1 + \dots + e_n)$ is not an idempotent, i.e.

$$1 - (e_1 + \dots + e_n) = 0$$

whence $e_1 + \dots + e_n = 1$. □

Theorem 2.7

Let M be a finite meadow and $\{e_1, \dots, e_n\} \subseteq M$ the set of minimal idempotents. Then

$$M \cong e_1 \cdot M \times \dots \times e_n \cdot M$$

Proof: Because the theory of meadows is equational, we know from universal algebra that a direct product of meadows is a meadow. Thus $e_1 \cdot M \times \cdots \times e_n \cdot M$ is a meadow with multiplicative identity element (e_1, \dots, e_n) and the operations defined componentwise. Define $h : M \rightarrow e_1 \cdot M \times \cdots \times e_n \cdot M$ by

$$h(m) = (e_1 \cdot m, \dots, e_n \cdot m).$$

Then h is a homomorphism. Suppose $h(m) = h(m')$. Then for every $1 \leq i \leq n$, $e_i \cdot m = e_i \cdot m'$. Thus

$$\begin{aligned} m &= 1 \cdot m = (e_1 + \cdots + e_n) \cdot m \\ &= e_1 \cdot m + \cdots + e_n \cdot m \\ &= e_1 \cdot m' + \cdots + e_n \cdot m' \\ &= (e_1 + \cdots + e_n) \cdot m' = 1 \cdot m' = m'. \end{aligned}$$

Hence h is injective. Now let $(e_1 \cdot m_1, \dots, e_n \cdot m_n) \in e_1 \cdot M \times \cdots \times e_n \cdot M$ and consider $m = e_1 \cdot m_1 + \cdots + e_n \cdot m_n$. Then, since e_i and e_j are orthogonal for $i \neq j$, $e_i \cdot m = e_i \cdot m_i$. Thus $h(m) = (e_1 \cdot m_1, \dots, e_n \cdot m_n)$. Whence h is also surjective. \square

The order, or number of elements, of finite fields is of the form p^n , where p is a prime number. Since any two finite fields with the same number of elements are isomorphic, there is a naming scheme of finite fields that specifies only the order of the field. One notation for a finite field—or more precisely, its zero-totalized expansion, in which inverse is a total operation with $0^{-1} = 0$ —with p^n elements is $GF(p^n)$, where the letters GF stand for *Galois field*. From the above theorem it now follows immediately that the class of finite meadows is the closure of the class of Galois fields under finite products.

Corollary 2.8

Let $\Sigma = \{0, 1, +, -, \cdot, ^{-1}\}$ and M be a finite Σ -structure with cardinality n . Then M is a meadow if and only if there are—not necessarily distinct—primes p_1, \dots, p_k and natural numbers n_1, \dots, n_k such that

$$M \cong GF(p_1^{n_1}) \times \cdots \times GF(p_k^{n_k})$$

and $n = p_1^{n_1} \cdots p_k^{n_k}$.

Observe that—as a consequence—meadows of the same size are not necessarily isomorphic: $GF(4)$ and $GF(2) \times GF(2)$ are both meadows but $GF(4) \not\cong GF(2) \times GF(2)$. However, minimal finite meadows—i.e. meadows containing no proper submeadows—of the same size are isomorphic.

Corollary 2.9

(1) Let M be a finite minimal meadow with cardinality n . Then there are

distinct primes p_1, \dots, p_k such that

$$M \cong \mathbb{Z}/p_1\mathbb{Z} \times \dots \times \mathbb{Z}/p_k\mathbb{Z}$$

and $n = p_1 \cdots p_k$.

(2) Finite minimal meadows of the same size are isomorphic.

Proof: (2) follows from (1) and (1) follows from the preceding corollary and the fact that every minimal meadow has n elements, where n is squarefree, i.e. its prime factor decomposition is the product of distinct primes (cf. [1]).
□

As an application of Corollary 2.8, we determine the number of self-inverse and invertible elements in finite meadows.

Definition 2.10 Let $M = \langle M, 0, 1, +, -, \cdot, {}^{-1} \rangle$ be a meadow and $m \in M$. Then

- (1) m is self-inverse if $m = m^{-1}$,
- (2) m is invertible if $m \cdot m^{-1} = 1$,

So, e.g. in $\mathbb{Z}/10\mathbb{Z}$ (see Example 1.1) 0, 1, 4, 5, 6 are self-inverse elements, 1, 3, 7, are invertibles, and 9 is both self-inverse and invertible.

Proposition 2.11

Let $M \cong GF(p_1^{k_1}) \times \dots \times GF(p_n^{k_n})$. Then M has

- (1) $2^l \cdot 3^{n-l}$ self-inverses, where $l = |\{i \mid 1 \leq i \leq n \text{ \& } p_i = 2 \text{ \& } k_i = 1\}|$, and
- (2) $(p_1^{k_1} - 1) \cdots (p_n^{k_n} - 1)$ invertibles.

Proof: First observe that the number of self-inverses [invertibles] of M is the product of the number of self-inverses [invertibles] in the Galois fields.

(1) Now m is self-inverse in a meadow iff $m^3 = m \cdot m \cdot m^{-1} = m$. Thus the number of self-inverses in $GF(p_i^{k_i})$ is the number of elements such that $m \cdot (m - 1) \cdot (m + 1) = 0$. Since a field has no zero divisors, these are precisely the elements 0, 1 and -1 . Thus if $p_i = 2$ and $k_i = 1$ then $GF(p_i^{k_i})$ has 2 self-inverses and otherwise 3.

(3) Since in a field every element is invertible except 0, $GF(p_i^{k_i})$ has $p_i^{k_i} - 1$ invertibles. □

Acknowledgement: We are indebted to one of the referees of an earlier version of this paper who observed that our results on invertibles and self-inverses are simple corollaries of the Chinese Remainder Theorem and ring decomposition.

References

- [1] J.A. Bergstra, Y. Hirschfeld, and J.V. Tucker. *Meadows*, report PRG0705, September 2007.
(available from www.science.uva.nl/research/prog/publications.html).
- [2] J.A. Bergstra and J.V. Tucker. The Rational Numbers as an Abstract Data Type. *Journal of the ACM*, 54(2), April, 2007.
- [3] G. Birkhoff. Subdirect unions in universal algebra. *Bull. Amer. Math. Soc.*, 50(10):764–768, 1944.
- [4] D. Dolžan. Multiplicative sets of idempotents in a finite ring. *Journal of Algebra*, 304:271–277, 2006.
- [5] K.R. Goodearl. *Von Neumann Regular Rings*, Pitman, London, San-Francisco, Melbourne, 1979.